REMARKS

Claims 1-3, 5, 7-11, and 15-25 are pending in this application. By this Response, claims 1, 3, 5, 7, 11, 15 and 16 are amended, claims 4, 6, and 12-14 are canceled, and claims 17-25 are added. Independent claims 1, 7, 15, and 16 are amended to emphasize that the at least one publicly known constant is a constant selected from a set of publicly known constants that are used to implement the security function and that authentication is performed based on a message authentication code generated by the security function using the at least one selected publicly known constant. Support for these amendments may be found at least at page 3, line 32 to page 4, line 7 of the present specification. Claims 3, 5, and 11 are amended to be consistent with the amendments to their respective independent claims. Claim 11 is further amended to recite that the message authentication code (MAC) is generated as a hash of at least the message, the at least one publicly known constant, and a secret key. Support for the amendment to claim 11 may be found at least at page 4, line 29 to page 5, line 3 of the present specification. Claims 17-25 are added to recite additional features of the illustrative embodiments. Support for the addition of claims 17-25 may be found at least at page 3, line 32 to page 5, line 26 and of the present specification. Reconsideration of the claims is respectfully requested in view of the following remarks.

I. Telephone Interview

Applicants' representative contacted the Examiner to conduct a telephone interview prior to the response due date of the Office Action. However, due to the Examiner's schedule, a telephone interview was not able to be scheduled prior to the response due date. Therefore, Applicants respectfully request that the Examiner contact Applicants' representative to discuss this application prior to taking any further action on this case.

II. Objection to the Specification

The Office Action objects to the specification requiring clarification of the term "CBC-MAC" and "CBM-MAC." By this Response, the specification is amended to clarify these acronyms in the specification. Accordingly, Applicants respectfully request withdrawal of the objection to the specification.

III. Rejection under 35 U.S.C. § 112, Second Paragraph

The Office Action rejects claims 1-16 under 35 U.S.C. § 112, second paragraph. Specifically, the Office Action alleges that the term "the receiver" and "a target" in claim 1 is indefinite. Moreover, the Office Action alleges that the terms "the received message" and "the received publicly known constants" lack antecedent basis in claims 1, 15, and 16. Furthermore, the Office Action alleges that the terms "the secret key" and "the security function" in claim 12 lack antecedent basis.

By this Response, claims 1, 15, and 16 are amended to provide sufficient antecedent basis for all terms in these claims. Claim 1 is further amended to recite "a receiver" and "the receiver" with the elimination of the reference to "a target." Claim 12 is canceled by this Response. Thus, Applicants respectfully request withdrawal of the rejection of claims 1-16 under 35 U.S.C. § 112, second paragraph.

IV. Rejection under 35 U.S.C. § 102(b)

The Office Action rejects claims 1-4 and 7-16 under 35 U.S.C. § 102(b) as being allegedly anticipated by Connery et al. (U.S. Patent No. 6,311,276). This rejection is respectfully traversed.

Claim 1, which is representative of the other rejected independent claims 7 and 15-16 with regard to similarly recited subject matter, reads as follows:

> 1. A method for authenticating a message, comprising:
> performing a security function upon the message to generate a message authentication code, wherein the security function utilizes at least

one publicly known constant to perform the security function upon the message, and wherein the at least one publicly known constant is selected from a set of publicly known constants used to implement the security function;

sending the message to a receiver;

sending the message authentication code to the receiver; and

sending the at least one publicly known constant, used by the security function to perform the security function upon the message, to the receiver, wherein the receiver authenticates the received message based on the message authentication code and the at least one publicly known constant.

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). Applicants respectfully submit that Connery does not identically show every element of the claimed invention arranged as they are in the claims. Specifically, Connery does not teach the features of claim 1 emphasized above, or the similar features found in the other rejected independent claims.

Connery is directed to a mechanism for performing power management operations remotely, e.g., turning on/off a computing device remotely. The mechanism of Connery includes security logic that is responsive to data in a packet to authenticate the source of a message, to accept the message and generate a signal to a management circuit in the computing device when the message passes authentication (see Abstract). The message may contain a timestamp, a random value token, and a message authentication code (column 7, lines 32-38). The timestamp is a 32 bit value indicating the time at which the message was generated (column 8, lines 13-15). The timestamp may be used as a mechanism for ensuring that the message is not reused (column 2, lines 51-64) and to remove random numbers from a replay cache (column 8, lines 18-22). The random value token may also be used to ensure that a message is not reused. The

message authentication code is a cryptographic hash function using a secret key (column 7, lines 50-67) which is then authenticated at the end system.

While Connery teaches a message authentication code, Connery does not teach, or even suggest, that the security function utilizes at least one publicly known constant to perform the security function upon the message, the at least one publicly known constant being selected from a set of publicly known constants used to implement the security function, and sending the at least one publicly known constant to the receiver which uses it to authenticate the message. To the contrary, in Connery, only the timestamp, random value token, and message authentication code are transmitted to the end system as parameters. Neither the timestamp nor the random value token are used to perform the cryptographic hash function to generate the message authentication code. Thus, Connery does not teach that a publicly known constant, which is used to perform a security function on a message to generate a message authentication code, is sent to a receiver which uses it along with the message authentication code to authenticate the message.

The Office Action alleges that the timestamp in Connery is the same as the at least one publicly known constant. First, time is not a constant and thus, the timestamp cannot be considered a "publicly known constant." Second, and more importantly, even if the timestamp were considered to be a "constant," there is no teaching or even suggestion in Connery that the timestamp is used by the cryptographic hash function to generate the message authentication code. To the contrary, Connery only teaches using a secret key to perform a hash of the message itself. The timestamp is only used to ensure that the message is not reused.

Thus, Applicants respectfully submit that Connery does not teach each and every feature of independent claim 1, or the similar features found in the other independent claims 7 and 15-16, as is required under 35 U.S.C. § 102(b). At least by virtue of their dependency on claims 1 and 7, respectively, Connery does not teach each and every feature of dependent claims 2-3 and 8-11 (claims 4 and 12-14 having been canceled by this Response). Accordingly, Applicants respectfully request withdrawal of the rejection of claims 1-3, 7-11, and 15-16 under 35 U.S.C. § 102(b).

In addition to the above, with regard to claim 11, Connery does not teach, or even suggest, that a message authentication code (MAC) is generated as a hash of at least the

message, the at least one publicly known constant, and a secret key. Connery teaches that the message authentication code is generated as a hash of the message using a secret key. However, Connery does not teach or suggest that the hash function hashes the message, the secret key, **and** at least one publicly known constant to generate the message authentication code. Thus, in addition to its dependency on claim 7, Connery does not teach the specific features set forth in claim 11.

V. Rejection under 35 U.S.C. § 103(a)

The Office Action rejects claims 5 and 6 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Connery in view of Sibert (U.S. Patent No. 6,832,316). This rejection is respectfully traversed.

By this Response, the features of claim 6 are combined with the features of claim 5 and thus, this Response will address only amended claim 5. While Sibert may teach an encryption and decryption function, Sibert does not provide any teaching or suggestion to compensate for the deficiencies of Connery noted above with regard to the rejection under 35 U.S.C. §102(b). That is, as with Connery, Sibert does not teach or suggest the sending of the at least one publicly known constants to the receiver which uses the at least one publicly known constants along with the message authentication code to authenticate the message. Thus, even if Sibert is combinable with Connery, arguendo, the result still would not obviate the invention recited in independent claim 1 from which claim 5 depends. Accordingly, Applicants respectfully request withdrawal of the rejection of claim 5 under 35 U.S.C. § 103(a).

VI. Newly Added Claims 17-25

Claims 17-25 are added to recite additional features of the invention. Claims 17 and 22 are added to recite that the security function is a Secure Hash Algorithm (SHA) and the set of publicly known constants comprises the first 64 bits of the fractional parts of the cube roots of the first eighty prime numbers. While Connery mentions SHA (column 7, lines 50-68), nowhere does Connery teach or suggest that the set of publicly

known constants, from which at least one publicly known constant is selected, are the first 64 bits of the fractional parts of the cube roots of the first eighty prime numbers. Moreover, Sibert does not teach or suggest this feature either. Thus, neither Connery nor Sibert, either alone or in combination, teach or suggest that the at least one publicly known constant that is sent to the receiver is one of these values.

Claim 18 is added to recite that the receiver does not store the set of publicly known constants. As discussed in the present specification, prior to the present invention, recipient computing devices were required to store the entire set of publicly known constants if they were to implement a particular security function. With the invention as recited in claim 18, the recipient computing device does not store the set of publicly known constants but is still able to implement the security function to perform authentication since the at least one publicly known constant used by the security function to generate the message authentication code is sent to the recipient computing device. No such feature is taught or suggested by either Connery or Sibert.

Claims 19 and 23 are added to recite authenticating the message as a function of at least a shared key, the at least one publicly known constant, the security function, the message, and the message authentication code. While Connery teaches to authenticate the message based on the message authentication code and the secret key, nowhere does Connery teach or suggest to authenticate the message as a function of at least a shared key, the at least one publicly known constant, the security function, the message, and the message authentication code.

Claims 20 and 24 are added to recite computing a second media access code based on the received at least one publicly known constant, the received message, and a secret key stored by the receiver, comparing the second media access code to the received media access code, and determining that the received message is authentic in response to the second media access code matching the received media access code. Neither Connery nor Sibert teach or suggest these features for similar reasons as noted above.

Claims 21 and 25 are added to recite that the hash function is applied to a secret key, the at least one publicly known constant, and the message such that the resulting message authentication code is equal to a hash of the combination of the secret key, the at least one publicly known constant, and the message. These features are similar to the

features of claim 11 and thus, distinguish over Connery and Sibert for similar reasons as noted above with regard to claim 11. Prompt and favorable consideration of claims 17-25 is respectfully requested.

VII. Conclusion

It is respectfully urged that the subject application is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

DATE: September 27, 2007

Stephen J. Walder, Jr.
Reg. No. 41,534
WALDER INTELLECTUAL PROPERTY LAW, P.C.
P.O. Box 832745
Richardson, TX 75083
(214) 722-6419
ATTORNEY FOR APPLICANTS